ブーリアングレブナ基底を使った数独の解法 (Computer Algebra : Design of Algorithms, Implementations and Applications)

AUTHOR(S):

井上, 秀太郎; 佐藤, 洋祐; 鈴木, 晃; 鍋島, 克輔

CITATION:

井上, 秀太郎 ...[et al]. ブーリアングレブナ基底を使った数独の解法 (Computer Algebra : Design of Algorithms, Implementations and Applications). 数理解析研究所講究録 2009, 1666: 1-5

ISSUE DATE:

2009-10

URL:

http://hdl.handle.net/2433/141086

数理解析研究所講究録
第1666巻 2009年 1-5

ブーリアングレブナ基底を使った数独の解法

井上　秀太郎
SHUTARO INOUE
東京理科大学大学院理学研究科
GRADUATE SCHOOL OF SCIENCE, TOKYO UNIVERSITY OF SCIENCE*

佐藤　洋祐
YOSUKE SATO
東京理科大学理学部
DEPARTMENT OF MATHEMATICAL INFORMATION SCIENCE, TOKYO UNIVERSITY OF SCIENCE†

鈴木 晃
AKIRA SUZUKI
神戸大学情報管理室
OFFICE OF INFORMATION MANAGEMENT, KOBE UNIVERSITY‡

鍋島 克輔
KATSUSUKE NABESHIMA
大阪大学大学院情報科学研究科
GRADUATE SCHOOL OF INFORMATION SCIENCE AND TECHNOLOGY, OSAKA UNIVERSITY§

1　はじめに

数独とは世界的に有名なパズルの一つである. 数独に関する研究はいくつか存在するが, ブール環を利用した研究は存在しない. そこで本研究ではブーリアングレブナ基底を使用した数独の解法を提案する.

2　ブール多項式環

ブール環とブール多項式環を次のように定義する.

定義 1 全ての要素が冪等であるような、単位元をもつ可換環 $\mathbf{B}$ をブール環とよぶ.

*j1106701@ed.kagu.tus.ac.jp
†ysato@rs.kagu.tus.ac.jp
‡sakira@kobe-u.ac.jp
§nabeshima@math.sci.osaka-u.ac.jp

定義 2 ブール環 $\mathbf{B}$ を係数とする多項式環 $\mathbf{B}[X_1,\ldots,X_n]$ のイデアル $\langle X_1^2-X_1,\ldots,X_n^2-X_n\rangle$ による剰余環をブール多項式環とよび、$\mathbf{B}(X_1,\ldots,X_n)$ で表す.

ブール多項式に関しては拡張定理と零点定理が成り立つ.

定理 1 (拡張定理) I をブール多項式環 $\mathbf{B}(\bar{A},\bar{X})$ のイデアルとする. このとき任意の $\bar{a}\in V(I\cap\mathbf{B}(\bar{X}))$ にたいして $(\bar{a},\bar{b})\in V(I)$ となる $\bar{b}$ が存在する.

定理 2 (零点定理) I をブール多項式環 $\mathbf{B}(\bar{X})$ のイデアルとする. このとき

$$V(I)=\emptyset \Leftrightarrow \exists a\in\mathbf{B}\ a\in I \quad (\text{弱形の零点定理})$$

が成り立つ. また I が有限生成であると仮定する. このとき

$$f(\bar{X})\in I \Leftrightarrow \forall\bar{a}\in V(I)\ f(\bar{a})=0 \quad (\text{強形の零点定理})$$

が成り立つ.

3 ブーリアングレブナ基底

まず始めに係数ブール環上の多項式環でのグレブナ基底について説明する. 以降は次の記号を使用する. ある順序に対してブール多項式 f の最大の単項式を $LM(f)$ で表し,$LM(f)$ の係数と項をそれぞれ $LC(f)$ と $LT(f)$ で表す. また $f-LM(f)$ を $Rd(f)$ で表す.

定義 3 ブール多項式環 $\mathbf{B}[\bar{X}]$ のイデアル I に対して,I の有限部分集合 G が I のグレブナ基底であるとは $\langle LM(I)\rangle=\langle LM(G)\rangle$ を満たすことである.

定義 4 ブール多項式 $f=a\alpha+h\in\mathbf{B}[\bar{X}]$ による単項式簡約 $\rightarrow_f$ を

$$b\alpha\beta\rightarrow_f b(1+a)\alpha\beta+ba\beta h$$

と定義する.
(ただし $a=LC(f),b\in\mathbf{B},ab\neq 0$ とし,$\alpha=LT(f),\beta\in T(\bar{X}),h=Rd(f)$ とする.)

係数ブール環上のグレブナ基底の計算には次の定義が必要になる.

定義 5 多項式 f が $lc(f)f=f$ を満たすとき f はブール閉であるという. $lc(f)f$ を f のブール閉包とよび、$bc(f)$ で表す.

一般の係数体のときと違い, 簡約グレブナ基底は一意性をもたない. よって新しい条件を加える.

定義 6 G を既約グレブナ基底とする. 任意の異なる多項式 $f,g\in G$ にたいして $LT(f)\neq LT(g)$ が成り立つとき G は *stratified* であるとよぶ.

定理 3 G,H を $\langle G\rangle=\langle H\rangle$ を満たす *stratified* なグレブナ基底であるとする. このとき $G=H$ が成り立つ.

係数ブール環上のグレブナ基底は上記の単項式簡約を利用したブッフバーガーアルゴリズムで計算できる.

Algoritm BC
Input: F a finite subset of $\mathbf{B}[\bar{X}]$
Output: F' a set of boolean closed polynomials such that $\langle F\rangle=\langle F'\rangle$

begin
$F' = \emptyset$
while $F \neq \emptyset$ do
　　select f from F
　　$F = F \backslash \{f\}$
　　$F' = F' \cup \{bc(f)\}$
　　$F = F \cup \{f - bc(f)\}$
end
return F'
　　Algoritm GB
Input: F a finite subset of $\mathbf{B}[\bar{X}]$
Output: G a Gröbner basis of $\langle F \rangle$ w.r.t $>$
bigin
$G = BC(F)$
while
　　$G' = G$
　　for each pair $\{p, q\}(p, q \in G', p \neq q)$ do
　　　　h = a normal form of $S(p, q)$ modulo G' i.e. $S(p, q) \xrightarrow{*}_G h$
　　　　if $h \neq 0$ then $G = G \cup \{h\}$
$G = G'$ do
end
ブーリアングレブナ基底に関しても今までの定義や定理と同じような議論ができる. またアルゴリズムも非常にシンプルである.

定義 7 ブール多項式環 $\mathbf{B}(\bar{X})$ のイデアル I に対して,I の有限部分集合 G が I のブーリアングレブナ基底であるとは $\langle LM(I) \rangle = \langle LM(G) \rangle$ を満たすことである.

　　Algoritm BGB
Input: F a finite subset of $\mathbf{B}(X_1, \ldots, X_n)$
Output: G a boolean Gröbner basis of $\langle F \rangle$ w.r.t $>$
begin
G =GB$(F \cup \{X_1^2 - X_1, \ldots, X_n^2 - X_n\})(X_1^2 - X_1, \ldots, X_n^2 - X_n \in \mathbf{B}[\bar{X}])$
$G = G \backslash \{X_1^2 - X_1, \ldots, X_n^2 - X_n\}$
end
return G

4　数独の解法

数独とは 9 × 9 ブロックの枠内に 1 から 9 までの数字をルールに従って入れるパズルである. 最も一般的なルールは次の 2 つである.、

1. 1 つのマスに 1〜9 の数字が 1 つ入る.
2. 縦, 横, 太線で囲まれた 3 × 3 ブロックに同じ数字は入れられない.

ブーリアングレブナ基底を使用するためにはこれらの条件を数式化する必要がある. その準備として 81 個の全ての枠に次の様な変数を割り当てる.

$x_{1,1}$	$x_{1,2}$	$x_{1,3}$	$x_{1,4}$	$x_{1,5}$	$x_{1,6}$	$x_{1,7}$	$x_{1,8}$	$x_{1,9}$
$x_{2,1}$	$x_{2,2}$	$x_{2,3}$	$x_{2,4}$	$x_{2,5}$	$x_{2,6}$	$x_{2,7}$	$x_{2,8}$	$x_{2,9}$
$x_{3,1}$	$x_{3,2}$	$x_{3,3}$	$x_{3,4}$	$x_{3,5}$	$x_{3,6}$	$x_{3,7}$	$x_{3,8}$	$x_{3,9}$
$x_{4,1}$	$x_{4,2}$	$x_{4,3}$	$x_{4,4}$	$x_{4,5}$	$x_{4,6}$	$x_{4,7}$	$x_{4,8}$	$x_{4,9}$
$x_{5,1}$	$x_{5,2}$	$x_{5,3}$	$x_{5,4}$	$x_{5,5}$	$x_{5,6}$	$x_{5,7}$	$x_{5,8}$	$x_{5,9}$
$x_{6,1}$	$x_{6,2}$	$x_{6,3}$	$x_{6,4}$	$x_{6,5}$	$x_{6,6}$	$x_{6,7}$	$x_{6,8}$	$x_{6,9}$
$x_{7,1}$	$x_{7,2}$	$x_{7,3}$	$x_{7,4}$	$x_{7,5}$	$x_{7,6}$	$x_{7,7}$	$x_{7,8}$	$x_{7,9}$
$x_{8,1}$	$x_{8,2}$	$x_{8,3}$	$x_{8,4}$	$x_{8,5}$	$x_{8,6}$	$x_{8,7}$	$x_{8,8}$	$x_{8,9}$
$x_{9,1}$	$x_{9,2}$	$x_{9,3}$	$x_{9,4}$	$x_{9,5}$	$x_{9,6}$	$x_{9,7}$	$x_{9,8}$	$x_{9,9}$

1 から 9 までの数字は集合の要素とする. つまり $S = \{1,2,3,4,5,6,7,8,9\}$ としたとき, 係数ブール環は $\mathbf{B} = \mathcal{P}(S) = \{A|A \subseteq S\}$ となる. 次に数独のルールをブール方程式で数式化するが, 簡単にするために次の枠に対する条件式について説明する.

$x_{1,1}$	$x_{1,2}$	$x_{1,3}$	$x_{1,4}$	$x_{1,5}$	$x_{1,6}$	$x_{1,7}$	$x_{1,8}$	$x_{1,9}$

1 から 9 の数字が 9 個の枠のどれかに入ることを次のブール方程式で表す.

$$x_{1,1} + x_{1,2} + x_{1,3} + x_{1,4} + x_{1,5} + x_{1,6} + x_{1,7} + x_{1,8} + x_{1,9} = \{1,2,3,4,5,6,7,8,9\}$$

違う枠に同じ数字が入らないことを次のブール方程式で表す.

$x_{1,1}x_{1,2} = 0, x_{1,1}x_{1,3} = 0, x_{1,1}x_{1,4} = 0, x_{1,1}x_{1,5} = 0, x_{1,1}x_{1,6} = 0, x_{1,1}x_{1,7} = 0, x_{1,1}x_{1,8} = 0, x_{1,1}x_{1,9} = 0,$
$x_{1,2}x_{1,3} = 0, x_{1,2}x_{1,4} = 0, x_{1,2}x_{1,5} = 0, x_{1,2}x_{1,6} = 0, x_{1,2}x_{1,7} = 0, x_{1,2}x_{1,8} = 0, x_{1,2}x_{1,9} = 0,$
$x_{1,3}x_{1,4} = 0, x_{1,3}x_{1,5} = 0, x_{1,3}x_{1,6} = 0, x_{1,3}x_{1,7} = 0, x_{1,3}x_{1,8} = 0, x_{1,3}x_{1,9} = 0,$
$x_{1,4}x_{1,5} = 0, x_{1,4}x_{1,6} = 0, x_{1,4}x_{1,7} = 0, x_{1,4}x_{1,8} = 0, x_{1,4}x_{1,9} = 0,$
$x_{1,5}x_{1,6} = 0, x_{1,5}x_{1,7} = 0, x_{1,5}x_{1,8} = 0, x_{1,5}x_{1,9} = 0,$
$x_{1,6}x_{1,7} = 0, x_{1,6}x_{1,8} = 0, x_{1,6}x_{1,9} = 0,$
$x_{1,7}x_{1,8} = 0, x_{1,7}x_{1,9} = 0,$
$x_{1,8}x_{1,9} = 0$

数独のルールから上記の方程式が 27 組必要となる. 次に数独の問題として最初に与えられる数字をブール方程式で表す必要がある. これは $x_{i,j}$ の枠に数字 e が入っていた場合,$x_{i,j} = \{e\}$ と表す.$(i,j,e = 1,\ldots,9)$ 例えば $x_{1,5}$ の枠に 2 が入っていた場合は $x_{1,5} = \{2\}$ となる. 上記のブール方程式をブール多項式として, 辞書式順序でブーリアングレブナ基底の計算を行う. ここで重要となるのは得られたブーリアングレブナ基底が数独としての解になっていないことである. 拡張定理より解の存在は保証されているが, 数独の解であるかどうかは確かめる必要がある. 確かめる方法は場合分けと後退代入を繰り返しである. 辞書式順序で計算しているので, ブーリアングレブナ基底から変数順序の低い変数から生成される多項式を取り出せる. よって順番に後退代入を行うことで効率のよい計算ができる.

5 まとめ

Risa/Asir で実装した数独解答プログラムによる計算実験の結果から, 計算時間では既存のプログラムより劣ることがわかった. 今回の方法はブーリアングレブナ基底を使用することである程度まで空枠の数字の候補を絞っているだけである. 単純な全解探索より効率的であるが, まだまだ無駄な計算も多いのが現状で

ある．しかし今回の方法の改良としてブーリアングレブナ基底の計算を繰り返すだけで数独の解を求める方法を研究中である．この方法は繰り返しの過程で変数の個数が減り，場合分けが少ない等の有利な点が多い．

参 考 文 献

[1] Sato, Y. et al.(1996). Set Constrains Solvers(Prolog version). http://www.icot.or.jp/ARCHIVE/Museum/FUNDING/funding-96-E.html

[2] Sato, Y.(1998). A new type of canonical Gröbner bases in polynomial rings over Von Neumann regular rings. Proceedings of ISSAC 1998, ACM Press, pp 317-32.

[3] Sato, Y. et al.(1998). Set Constrains Solvers(Klic version). http://www.icot.or.jp/ARCHIVE/Museum/FUNDING/funding-98-E.html

[4] Sato, Y. and Inoue, S.(2005). On the Construction of Comprehensive Boolean Gröbner Bases. Proceedings of the Seventh Asian Symposium on Computer Mathematics(ASCM 2005), pp 145-148.

[5] Sato, Y., Inoue, S., Suzuki, A. and Nabeshima, K. Boolean Gröbner Bases and Sudoku. Submitted for publication.

[6] Sato, Y., Nagai, A. and Inoue, I.(2008). On the Computation of Elimination Ideals of Boolean Polynomial Rings, LNAI 5081, pp 338-348, Springer-Verlag Berlin Heidelberg.

[7] Sakai, K. and Sato, Y. (1988). Boolean Gröbner bases. ICOT Technical Momorandum 488. http://www.icot.or.jp/ARCHIVE/Museum/TRTM/tm-list-E.html

[8] Sakai, K., Sato, Y. and Menju, S. (1991). Boolean Gröbner bases(revised). ICOT Technical Report 613. http://www.icot.or.jp/ARCHIVE/Museum/TRTM/tr-list-E.html

[9] Sato, Y. and Suzuki, A. (1999). Parallel computation of BooleanGrbner Bases. Proceedings of the Fourth Asian Technology Conference in Mathematics(ATCM 1999), pp 265-274.